

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF:
218-57 139TH AVENUE, SPRINGFIELD
GARDENS, NEW YORK

**APPLICATION FOR A SEARCH
WARRANT FOR A PREMISES**

No. 18-mj-293

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Mark I. Rubins, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 218-57 139th Avenue, Springfield Gardens, New York, 11413, hereinafter “SUBJECT RESIDENCE,” further described in Attachment A, for all credit, debit, or prepay cards in the possession or name of RICARDO and ROJAY STAMP.

2. I am a Detective with the New York City Police Department (“NYPD”) and have been since 2013. Since 2017, I have been assigned to the Cybercrime Task Force at the Federal Bureau of Investigation (“FBI”). I am responsible for conducting and assisting in investigations involving cybercrime. I have investigated and otherwise participated in numerous matters during the course of which I have conducted physical surveillance, interviewed witnesses, executed court-authorized search warrants and used other investigative techniques to secure relevant information. I am familiar with the facts and circumstances set forth below from my

participation in the investigation, my review of the investigative file, and from reports of witnesses and other law enforcement officers involved in the investigation.

3. As set forth below, there is probable cause to believe that the SUBJECT RESIDENCE contains evidence of violations of Title 18, United States Code, Sections 1029 (access device fraud); 1030 (fraud and related activity in connection with computers), 1343 (wire fraud), and 1344 (bank fraud). More specifically, there is probable cause to believe that numerous credit cards belonging to RICARDO STAMP at the SUBJECT RESIDENCE were used to steal customers' payment card information.

PROBABLE CAUSE

4. Based on my and other agents' review of the complaint, server logs, and malware provided by Amazing Grass; subscriber records and publicly available records relied upon by cyber investigators; and my knowledge, training, and experience, I know the following:

A. In Fall 2017, a UI Hacked Amazing Grass

5. Grass Advantage LLC, dba Amazing Grass, dba amazinggrass.com ("Amazing Grass") is located in Newport Beach, California. Through its website, amazinggrass.com, Amazing Grass sells plant-based nutrition products.

6. On November 22, 2017, the owner of Amazing Grass ("T.K."), submitted a written complaint to the FBI Internet Crime Complaint Center.

7. The complaint stated that an unknown individual (“UI”) had gained unauthorized access to Amazing Grass’s server and installed malware¹ designed to capture payment card information. The complaint reported that between September 11, 2017 and November 3, 2017, the UI stole payment information belonging to approximately 1,180 online customers.

B. The Malware Exfiltrated Data to Three Domains

8. On December 13, 2017, T.K. provided the FBI a copy of the malware used to steal Amazing Grass’s data and server logs. Those items show that the malware sent payment card information from the Amazing Grass server to the following domains² (the “Domains”) on the dates indicated:

- a. shopsecureconnection.com (“Domain 1”), between September 11, 2017 and September 27, 2017;
- b. shopshieldsecure.com (“Domain 2”), between September 27, 2017 and October 16, 2017; and

¹ “Malware” is short for malicious software, which is an umbrella term used to refer to a variety of forms of harmful or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

² A “domain” is a distinct subset of the Internet with addresses sharing a common suffix or under the control of a particular organization or individual.

c. cdnspacconnection.com (“Domain 3”), between October 16, 2017 and November 3, 2017.

9. The FBI’s investigation into whether, and if so how and by whom, the information exfiltrated to the Domains was later accessed and used is ongoing. Based on my knowledge, training, and experience, however, hackers frequently use domains as an intermediary to their own computers to frustrate law enforcement efforts to identify them.

C. All of the Domains Were Registered From IP Addresses Located in Belgium

10. Centralops.net provides online tools for investigating, exploring, and troubleshooting Internet addresses such as domain names, IP addresses,³ email addresses, and Uniform Resource Locators (“URLs”), which are the names assigned to a domain to make it easier to remember (i.e., https://www.justice.gov, http://www.uscourts.gov, etc.). Centralops.net compiles publicly available domain registry records as part of the information it provides.

11. On December 14, 2017, an FBI agent conducted a search of centralops.net for the Domains. That search revealed that the Domains belonged to PublicDomainRegistry.com.

³ An Internet Protocol (“IP”) address is a unique string of numbers separated by periods that allows a computer to connect to the Internet.

12. PublicDomainRegistry.com provides domain registration services. In other words, it maintains a record of the URL associated with the IP address (or addresses) associated with a particular domain — that is, the IP address assigned to it in the DNS “phone book” when a computer on the internet looks up that domain.⁴

13. On December 21, 2017, PublicDomainRegistry.com provided the following registration information for the Domains:

Domain	Date Registered (2017)	Time Registered (GMT)	IP address Used to Access Registrant Account at Domain Service	Registrant Email Address
1	9/1	15:40:47	91.177.209.92	elsiepfox@myself.com
2	9/26	18:20:51	91.183.99.90	cliffordedensmore@protonmail.com
3	10/12	15:53:15	91.183.82.32	davidmhill@protonmail.com

⁴ The “Domain Name System,” or “DNS,” is a naming system for computers, services, or any other resources connected to the Internet. An often-used analogy to explain the DNS is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name “www.justice.gov” may translate to the IP address 149.101.146.50. An individual can register a domain (thus becoming its “registrant”) by paying a company known a domain name registrar. The registrant can control which IP address that domain will “point” to, i.e., which IP address is assigned to it in the “phone book.”

14. On December 21, 2017, an FBI agent conducted a search of centralops.net for the IP addresses identified in the table above and found that they all belong to Proximus NV in Belgium. Proximus Group provides telephony, Internet, television, and network-based information and communications technology services in Belgium through its Proximus and Scarlet brands.

D. A UI Accessed the Registrant Email Address for Domain 1 from an IP Address Associated With the SUBJECT RESIDENCE.

15. 1&1 Mail and Media, Inc. (“1&1”) hosts elsiepfox@myself.com, the registrant email address for Domain 1. Subscriber records provided by 1&1 show that the email address was registered at 15:26:29 GMT on September 1, 2017, approximately 14 minutes before Domain 1 was registered. The records also reflect that the email address elsiepfox@myself.com was registered by an Internet user who used the IP address 91.177.209.92—the same Belgium-located IP address used to register Domain 1.

16. However, according to records provided by 1&1, approximately four hours later the email address elsiepfox@myself.com was accessed from IP address 68.129.218.34, which is located in New York City (the “New York IP Address.”).

17. The New York IP Address belongs to a Verizon Fios account.. Verizon subscriber records for the New York IP Address show that it was registered to a Verizon Fios account under the name RICARDO STAMP (the “SUBSCRIBER”) at the SUBJECT

RESIDENCE between August 15, 2017 and October 30, 2017. The account was created on August 14, 2017 and registered to daytime telephone (929) 328-4309, evening telephone (516) 234-1651, and email address Mr.Stamp1992@gmail.com.

18. The Verizon subscriber records show that the New York IP address is a dynamic IP address, meaning one assigned to a particular account for a short period – in this case, between August 15, 2017 and October 30, 2017. As of January 8, 2017, the Verizon account belonging to the SUBJECT RESIDENCE remained registered to RICARDO STAMP.

E. Evidence of the Subject Offenses is Likely to Be Found in the Subject Residence

19. Based on my knowledge, training, and experience, I know that cyber criminals often use overseas IP addresses, especially IP addresses associated with virtual private networks (“VPNs”) or proxy servers, to hide their true identity. A VPN extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. One example of a VPN is when a user accesses a VPN server via an encrypted communication channel, and then accesses the Internet from that server, concealing his or her true “home” IP address (and thus location). Similarly, a proxy server is a dedicated computer or software system running on a computer that acts as an intermediary for requests from clients seeking resources from other servers, and similarly serves as a “relay” that conceals the user’s true home IP address.

20. The FBI is investigating whether the Belgian IP addresses belonged to a proxy or VPN service at the time of the exfiltration, or whether they are residential IP addresses like the one in New York that is the subject of this affidavit.

21. Based on my knowledge, training, and experience, I suspect that if those Belgian IP addresses did belong to a proxy or VPN service, then the presence of the New York IP Address in the account records of the email address used to register Domain 1 (i.e., elsiepfox@msyself.com) would strongly indicate that the proxy or VPN service momentarily failed, unmasking the true IP address of the UI responsible for registering Domain 1 (i.e., the New York IP Address).

F. The SUBSCRIBER to the New York IP Address Resides at the SUBJECT RESIDENCE

22. On January 10, 2018, an FBI agent conducted a database search for the SUBJECT RESIDENCE, which revealed the following individuals living at the residence:

a. RICARDO STAMP, DOB XX/XX/1992, telephone number (929) 328-4309, email address ricardostamp@yahoo.com. Notably, this is the daytime telephone number shown in the Verizon subscriber records for the SUBSCRIBER.

b. ROJAY STAMP, DOB XX/XX/1993, telephone number (516) 234-1651.

Notably, this is the evening telephone number shown in the Verizon subscriber records for the SUBSCRIBER.

c. BREANN STAMP, DOB XX/XX/1996, telephone number (347) 545-7794.

23. As of January 10, 2018, State of New York Department of Motor Vehicle records for RICARDO STAMP, ROJAY STAMP, and BREANN STAMP show the same three people resided at the SUBJECT RESIDENCE:

- a. RICARDO COLLIN STAMP, DOB XX/XX/1992, who resides at 218-57 139th Avenue, Jamaica, NY 11413. On January 31, 2018, an FBI agent conducted a search of Google for “218-57 139th Avenue, Jamaica, NY 11413,” which revealed it is alternate way of referencing the SUBJECT RESIDENCE.
- b. ROJAY DELANO STAMP, DOB XX/XX/1993, who resides at the SUBJECT RESIDENCE.
- c. BREANN STAMP, DOB XX/XX/1996, for whom there is no record on file.

24. On January 10, 2018, an FBI agent conducted an open source search for telephone number (929) 328-4309 and email address ricardostamp@yahoo.com, which revealed Facebook.com/ricardo.stamp, with the Facebook user-identification (“UID”) #100001662554124. The account was under the name “RICARDO STAMP” and the vanity photo section contained a video of an African American male saying that he lives in Queens, New York. Based on Google maps, the SUBJECT RESIDENCE is in Queens, New York.

25. On January 29, 2018, an Analyst at the United States Postal Inspection Service advised that as of that day, the following individuals were receiving mail at the SUBJECT RESIDENCE:

- a. RICARDO STAMP
- b. ROJAY STAMP
- c. BREANN STAMP
- d. WINSOME DAVIS
- e. GARY MIGNOTT
- f. SHERYL MIGNOTT

G. RICARDO and ROJAY STAMP's Facebook and Google Accounts Were Accessed from the New York IP Address During the Exfiltration

26. Google subscriber records for the email address Mr.Stamp1992@gmail.com (the same email address used to register the Verizon Fios account) show that it was registered to “Ricardo Stamp” and telephone number (929) 328-4309 (the same telephone number used to register the Verizon Fios account). The records also show that the email address was accessed from the New York IP Address at the following times during the exfiltration: September 7, 2017 23:48:55 UTC; September 7, 2017 at 23:42:42 UTC; September 13, 2017 at 03:23:51 UTC; and October 27, 2017 at 04:07:28 UTC.

27. Based on the following, I believe Daloopxiv@gmail.com belongs to and is used by ROJAY STAMP. Google subscriber records for account Daloopxiv@gmail.com show that it is registered to “Jay Hovee” and telephone number (516) 234-1651. Verizon subscriber records show that telephone number as the evening telephone number for the account providing Internet service to the SUBJECT RESIDENCE. That telephone number is also registered to the user of the free mobile video communications service Tango named “ROJAY STAMP,” and Daloopxiv@gmail.com is registered to an account on the social networking site AskFM which is subscribed to under the name “ROJAY STAMP.”

28. Google records show that Daloopxiv@gmail.com was accessed from the New York IP Address at the following times during the exfiltration: October 26, 2017 at 19:36:54 UTC; and September 1, 2017 08:26:51 UTC – the very same day elsiepfox@myself.com was accessed from the New York IP Address.

29. Facebook subscriber records for account 100001662554124 (“ricardo.stamp”) show that it was registered to telephone number (929) 328-4309 and accessed from the New York IP Address on the following dates near to and during the exfiltration: August 15, 2017 at UTC; August 18, 2017 at 03:57:10 UTC; August 25, 2017 at 20:11:39 UTC; October 30, 2017 at 02:58:52 UTC, and October 30, 2017 at 04:27:17 UTC.

H. RICARDO STAMP's Facebook Page Shows That He and His Sister BREANN STAMP Hacked Each Other's Facebook Accounts

30. On October 18, 2010, the user of the RICARDO STAMP Facebook account posted, "Because Breann Hacked & Thought this pic of Her big brother was cutee ❤<3 ❤<3 Ilu Twinn :)" above a picture of an African American male believed to be RICARDO STAMP. This post appears to show BREANN STAMP bragging that she hacked RICARDO STAMP's Facebook account and posted a picture of him that she liked.

31. On September 18, 2011, the user of the RICARDO STAMP account liked "Hacking Edge" (hackingedge.com).

a. On January 10, 2018, an FBI agent conducted a Google search of hackingedge.com. According to <https://hackingedgecom.wordpress.com>: "HackingEdge.com have the latest downloads for hacking programs you need. The group mainly concentrate (sic) on hot video games – like Maplestory, Combat Arms, Starcraft 2, Warcraft 3, and other famous ones (I can't cover everything)."

32. On December 23, 2011, the user of the RICARDO STAMP Facebook account posted, "hackes by ricardo's lil sister breann 😊(: ❤<3 rawr : * i love uu rick ❤", immediately followed by a post containing a photo of what appears to be BREANN STAMP with the caption, "my FAVORITE little sister ❤." Based on my knowledge, training, and

experience, I believe that this post shows that BREANN STAMP again hacked RICARDO STAMP's Facebook account and posted a picture of herself stating that she was RICARDO STAMP's favorite little sister. Although the posts reflect a joke between brother and sister RICARDO and BREANN STAMP, they also appear to demonstrate that BREANN STAMP knows how to gain unauthorized access to her brother's Facebook account.

33. The post had the following comments, which appear to confirm other's knowledge of BREANN STAMP's interest, and increased skill, at hacking:

Oswald Reid Jr: Yayyy good job....

Oswald Reid Jr: it's a good improvement huh

RICARDO STAMP: hey my Sister Breann Put this up I had no idea I had been hacked.

Oswald Reid Jr: lmao!!!! Yesssss

RICARDO STAMP: wait a min Yes what Ozzy

Oswald Reid Jr: lol she did it...good job bre!!

RICARDO STAMP: DONT ENCOURAGE HER

Oswald Reid Jr: why not lol

RICARDO STAMP: cuz she is EVIL and will do it again

34. On January 12, 2012, the user of the RICARDO STAMP Facebook account posted,

"hacked myy hiss favorite lil sister Bree : * ." Based on my knowledge, training, and experience, I believe that this post shows that RICARDO STAMP hacked the Facebook account belonging to BREANN STAMP in retaliation for her hacking his Facebook account. Once

again, although the posts seem to reflect a joke between brother and sister RICARDO and BREANN STAMP, it also appears to demonstrate that RICARDO STAMP knows how to gain unauthorized access to his sister's account.

35. Based on the above posts, I believe RICARDO STAMP had an interest in hacking video games in 2011. In addition, the evidence appears to show BREANN STAMP hacking RICARDO STAMP's Facebook account in December 2011 and then RICARDO STAMP posting that he hacked BREANN STAMP back in January 2012. Although the "hacks" were done in jest and several years ago, the evidence shows the interest and capability to "hack" by individuals believed to be living at the SUBJECT RESIDENCE.

I. Payment Card Information Stolen from Amazing Grass Has Been Used to Make Unauthorized Purchases

36. On December 29, 2017, a New York-resident victim of the Amazing Grace hack ("N.F.") sent the FBI a transaction history of online purchases made with her credit card ending in -8828, which is among the credit card numbers stolen from amazinggrass.com. The transactions include the following:

- a. November 21, 2017 purchase in the amount of \$21.59 from Amazing Grass. This appears to be the transaction by which Amazing Grass came into possession of N.F.'s credit card information.
- b. December 2, 2017 purchase in the amount of \$123.05 from Amer Sports.
- c. December 2, 2017 purchase in the amount of \$520.07 from J. Crew.

d. December 6, 2017 purchase in the amount of \$358.45 from Amer Sports.

J. The Subject Residence is Searched and Agents See Numerous Credit Cards with the Same Issuer and Cardholder

37. On March 6, 2018, United States Magistrate Judge Robert M. Levy, United States District Court for the Eastern District of New York, signed and authorized a search warrant for the SUBJECT PREMISES which was executed at approximately 6:00 a.m. on March 8, 2018. During the search, numerous electronic devices were seized including two routers. During the search, FBI agents discovered numerous credit/debit cards in a wallet RICARDO STAMP claimed was his, including:

a. Bank of America

- i. 4117 7339 8672 4506 - Valued Customer, Exp 10/2021
- ii. 4117 7339 7758 9314 - RICARDO STAMP, Exp 11/2020
- iii. 4943 4087 0001 4498 - RICARDO STAMP, Exp 11/2018
- iv. 4117 7339 7205 5931 - Valued Customer, Exp 04/2020
- v. 4117 7339 8735 9526 - RICARDO STAMP, Exp 11/2021
- vi. 4117 7339 7205 5931 - RICARDO STAMP, Exp 05/2020
- vii. 4117 7339 7521 4493 - RICARDO STAMP, Exp 08/2020
- viii. 4117 7339 7483 0059 - Valued Customer, Exp 08/2020

b. Capital One

- i. 5178 0593 0591 1647 - RICARDO C. STAMP, Exp 07/2021

- ii. 5108 0501 4202 7486 - RICARDO STAMP, Exp 04/2021
 - c. Credit One Bank
 - i. 4447 9623 5508 9925 - RICARDO STAMP, Exp 06/2020
 - d. Chase
 - i. 4368 8400 0265 0437 - COSI INC, Exp 01/2017
 - e. Unknown
 - i. 4403 9310 6920 4833 - RICARDO STAMP, Exp 02/2023
 - f. The wallet also contained a New York State Identification Card, #936014058, with the name "RICARDO COLLIN STAMP," DOB 12/16/1992, 21857 139th Avenue, Jamaica, NY 11413.
38. On March 8, 2018, RICARDO STAMP was interviewed by the FBI and provided the following information. The SUBJECT PREMISES had two routers, a Spectrum router used by the family and a Verizon Fios router almost exclusively used by RICARDO and ROJAY STAMP. The Verizon Fios wireless router had the following password, "Cantrcrackthispwboy." The exception was limited use by RICARDO STAMP's younger sister, BRIA IRVING. RICARDO STAMP also stated that he dropped out of high school after the eleventh grade and was unemployed. He had quit his job two weeks earlier as a server at Cosi, a restaurant located in Manhattan, New York. When asked about the numerous credit/debit cards found in his wallet, RICARDO STAMP said although there were a lot of credit/debit cards, they were for the same

account. RICARDO STAMP said he kept losing his credit/debit cards so requested replacements.

39. The FBI merely photographed the cards rather than seizing them, because the prior search warrant did not explicitly authorize the seizure of credit or debit cards. However, the FBI believes the credit/debit cards may contain critical evidence. Despite the cards' having RICARDO STAMP's name, the magnetic strip on the card may contain anyone's information, which would not be visible to a vendor swiping the card. If RICARDO STAMP presented one of the cards to a vendor, STAMP's identification documents would match the name written on the card, leading the vendor to conclude that the card was genuine—even if a victim's financial information was encoded on the magnetic strip. It is unlikely that RICARDO STAMP lost his Bank of America credit/debit card seven times and then found the lost card each time, resulting in his possession of eight Bank of America cards. In addition, RICARDO STAMP was in possession of a credit/debit card with the name "Cosi, Inc," the restaurant he no longer worked for. The FBI believes it is highly unlikely that RICARDO STAMP's previous employer authorized him to keep a company credit card.

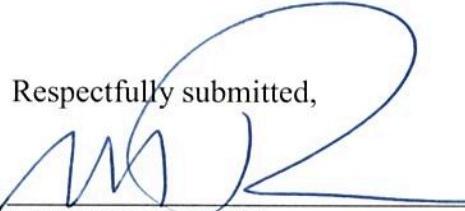
40. Furthermore, based on the evidence, ROJAY and RICARDO STAMP had almost exclusive access to the Verizon Fios router where the New York IP Address originated. Based on research by an FBI agent using a password calculator found at <https://www.logmeonce.com/password-calculator/>, the password "Canctrackthispwboy" would take 979 trillion years to hack. The FBI therefore believes it unlikely that anyone except

ROJAY, RICARDO and BRIA STAMP used the Verizon Fios router which accessed email address elsiepfox@myself.com the day it was created, which in turn was used to open up domain shopsecureconnection.com.

CONCLUSION

3. I submit that this affidavit supports probable cause for a warrant to search the SUBJECT RESIDENCE described in Attachment A and seize all credit, debit, or prepay cards in the possession or name of RICARDO and ROJAY STAMP.

Respectfully submitted,



MARK I. RUBINS
Detective
New York City Police Department

Subscribed and sworn to before me on April 5, 2018



Honorable Sanket J. Bulsara
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The premises located at 218-57 139th Avenue, Springfield Gardens, New York 11413 (“the SUBJECT RESIDENCE”), is located on a two-way street running approximately southeast to northwest. The bordering streets are Springfield Boulevard running north/south on the west side of the SUBJECT RESIDENCE and 219th Street running north/south to the east side of the SUBJECT RESIDENCE.

The SUBJECT RESIDENCE is a two-story home with light yellow or beige siding and white trim. The roof of the location is light grey and in visibly poor repair with missing shingles and a missing gutter. The roof of the SUBJECT RESIDENCE slopes away from the street. The front door faces the street and appears to be brown wood with an oval-shaped window in the center. The window extends most of the height of the door. The doorknob is on the left side of the door and there is a deadbolt above the doorknob. The residence has a porch fronted by dark colored painted brick. There are a total of four steps leading up to the front door and porch, and the porch is bordered by a black metal fence. There is a beige awning over the porch that is supported by three white metal lattices.

Directly to the left of the front door is a black metal mailbox. Above the mailbox are the numbers “218 57” in black lettering on a gold background.

ATTACHMENT B

Property to be seized

1. Any and all credit/debit cards under the name “RICARDO STAMP” or “ROJAY STAMP” including but not limited to the following cards:
 - a. Bank of America
 - i. 4117 7339 8672 4506 - Valued Customer, Exp 10/2021
 - ii. 4117 7339 7758 9314 - RICARDO STAMP, Exp 11/2020
 - iii. 4943 4087 0001 4498 - RICARDO STAMP, Exp 11/2018
 - iv. 4117 7339 7205 5931 - Valued Customer, Exp 04/2020
 - v. 4117 7339 8735 9526 - RICARDO STAMP, Exp 11/2021
 - vi. 4117 7339 7205 5931 - RICARDO STAMP, Exp 05/2020
 - vii. 4117 7339 7521 4493 - RICARDO STAMP, Exp 08/2020
 - viii. 4117 7339 7483 0059 - Valued Customer, Exp 08/2020
 - b. Capital One
 - i. 5178 0593 0591 1647 - RICARDO C. STAMP, Exp 07/2021
 - ii. 5108 0501 4202 7486 - RICARDO STAMP, Exp 04/2021
 - c. Credit One Bank
 - i. 4447 9623 5508 9925 - RICARDO STAMP, Exp 06/2020
 - d. Chase
 - i. 4368 8400 0265 0437 - COSI INC, Exp 01/2017

e. Unknown Issuer

i. 4403 9310 6920 4833 - RICARDO STAMP, Exp 02/2023